3.6 Security Management

3.6.1 Security Management Login Failure Scenario

3.6.1.1 Scenario Description

This scenario describes the steps that are that involved in monitoring a login failure. In this example, there are a variety of different ECS personnel involved. The definitions and roles of the participating staff members are taken from the Maintenance and Operations Manual for the ECS Project 607-CD-001-001) and/or The Maintenance and Operations Configuration Management Plan for the ECS Project. The personnel involved are, sustaining engineer, resource manager and host operator. In the beginning of the scenario a user attempts to unsuccessfully login three times. On the third incorrect login attempts, a security event is send to security monitor. Computer operator is notified of the security event and pinpoints the specifics using HP OpenView. Computer operator realizing that a violation has occurred, forwards the information to the SMC security controller.

3.6.1.2 Frequency

Security tests are run on a scheduled basis, and on-demand at the request of the site M&O staff, in order to audit the implementation of the security mechanisms.

3.6.1.3 Assumptions

The assumptions underlying this scenario are as follows:

1. Policy received from the SMC security controller has been implemented.
2. Release A, only operators have login accounts that directly log into ECS.
3. Registered Users log into the Client on their desktop.
4. The User has already failed his log in three times.

3.6.1.4 Components

Figure 3.6.1.4-1 indicates the interaction between the DAAC personnel and the ECS subsystems.

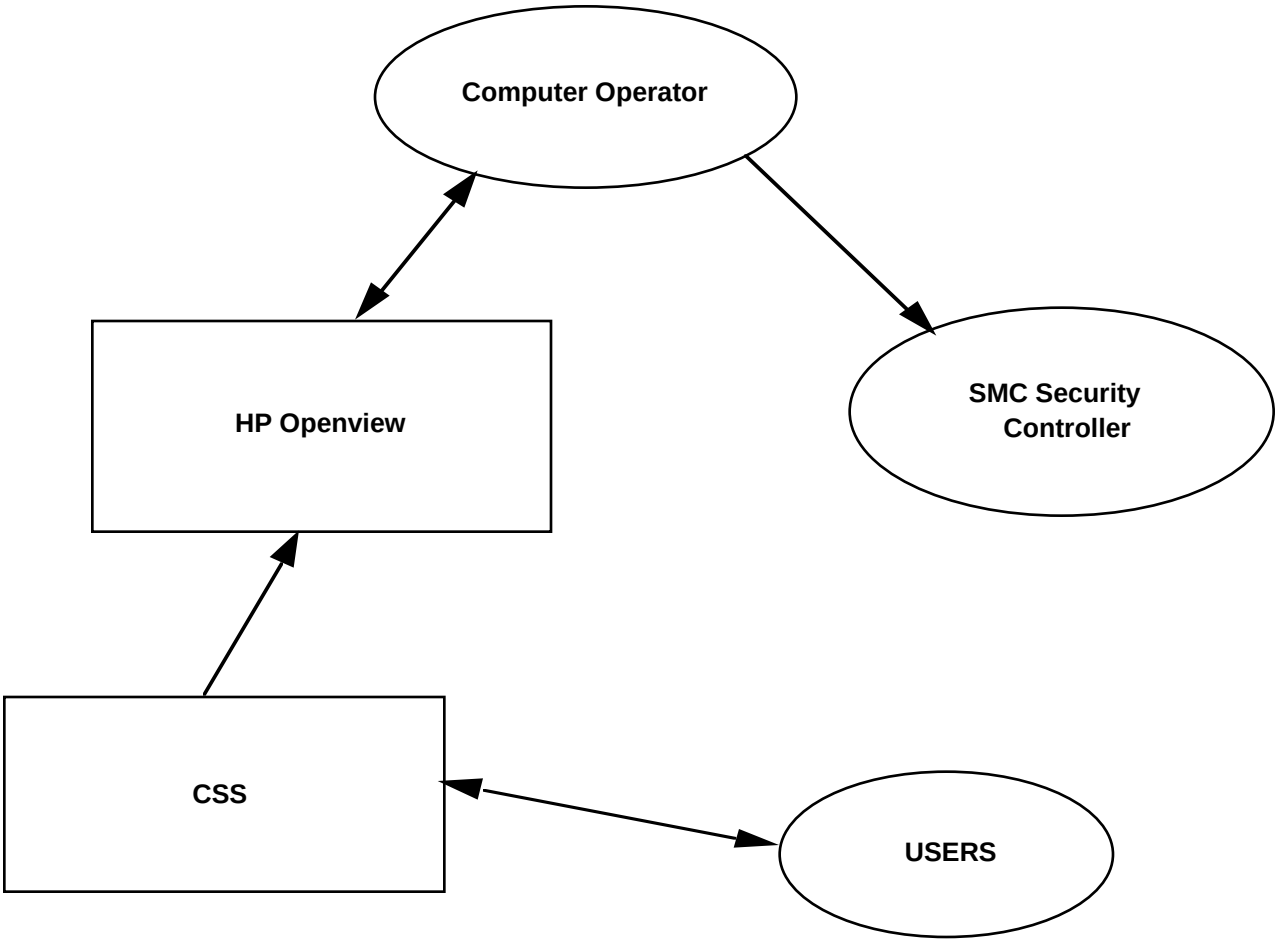

Figure 3.6.1.4-1. Security Management Login Failure Components

3.6.1.5 Preconditions

The preconditions underlying this scenario are:

1. The number of failed login attempts before the event is sent to the SMC is a DAAC configurable parameter.

3.6.1.6 Detailed Steps of Process

Table 3.6.1.6-1 represents the details of this scenario. The times and duration given are approximate.

Table 3.6.1.6-1. Security Management Login Failure Process (1 of 2)

Step	Duration	User	Operator	System	Figure
1	<1 Time = 0800		DAAC User Assistant incorrectly types in an incorrect password.	Rejects user login, logs event to DCE log files.	
2	<1 Time = 0801		DAAC User Assistant incorrectly types in an incorrect password.	Rejects user login, logs event to DCE log files.	
3	<1 Time = 0802		DAAC User Assistant incorrectly types in an incorrect password.	Lock the login station, lock the user account, logs event to DCE log files, send security event to security management monitor	
4	2 Time = 0803		Computer operator is notified of the security event.		
5	10 Time = 0805		computer operator view the event log through HP OpenView.		
6	1 Time = 0815		computer operator single clicks on the GSFC icon.		3.6.1.6-1
7	1 Time = 0816		computer operator selects the Security Events option from the Event Categories Window.	The system initializes the Event Browser listing all of the Security Events that have occurred.	3.6.1.6-2
8	1 Time = 0817		Computer Operator browses the information to determine how often the threat is occurring.		3.6.1.6-3
9	5 Time = 0818		computer operator calls the DAAC User Assistant to investigate the cause of the incorrect logins.		

10	5 Time = 0823		The DAAC User Assistant says that he can not remember his password and asks the Computer Operator if he could reset his account with a temporary password.		
11	2 Time = 0828		Computer Operator resets the DAAC User Assistants account.		

Step	Duration	User	Operator	System	Figure
12	1 Time = 0830		Computer Operator notifies the DAAC User Assistant that his password has been set and the first time he logs onto the system he will have to reset his password.		
13	<1 Time = 0831		DAAC User Assistant logs into ECS with the new password.		
14	<1 Time = 0832			System prompts the DAAC User Assistant to enter a new password.	
15	<1 Time = 0833		DAAC User Assistant enters new password		
16	<1 Time = 0834			System prompts the DAAC User Assistant to reenter the password.	
17	<1 Time = 0835		DAAC User Assistant reenters new password		
18	<1 Time = 0836			System sets new password.	
19	Time = 0837		DAAC User Assistant is free to continue working as usual.		

3.6.1.7 Postconditions

The DAAC User Assistant has a new password and the security event has been cleared.

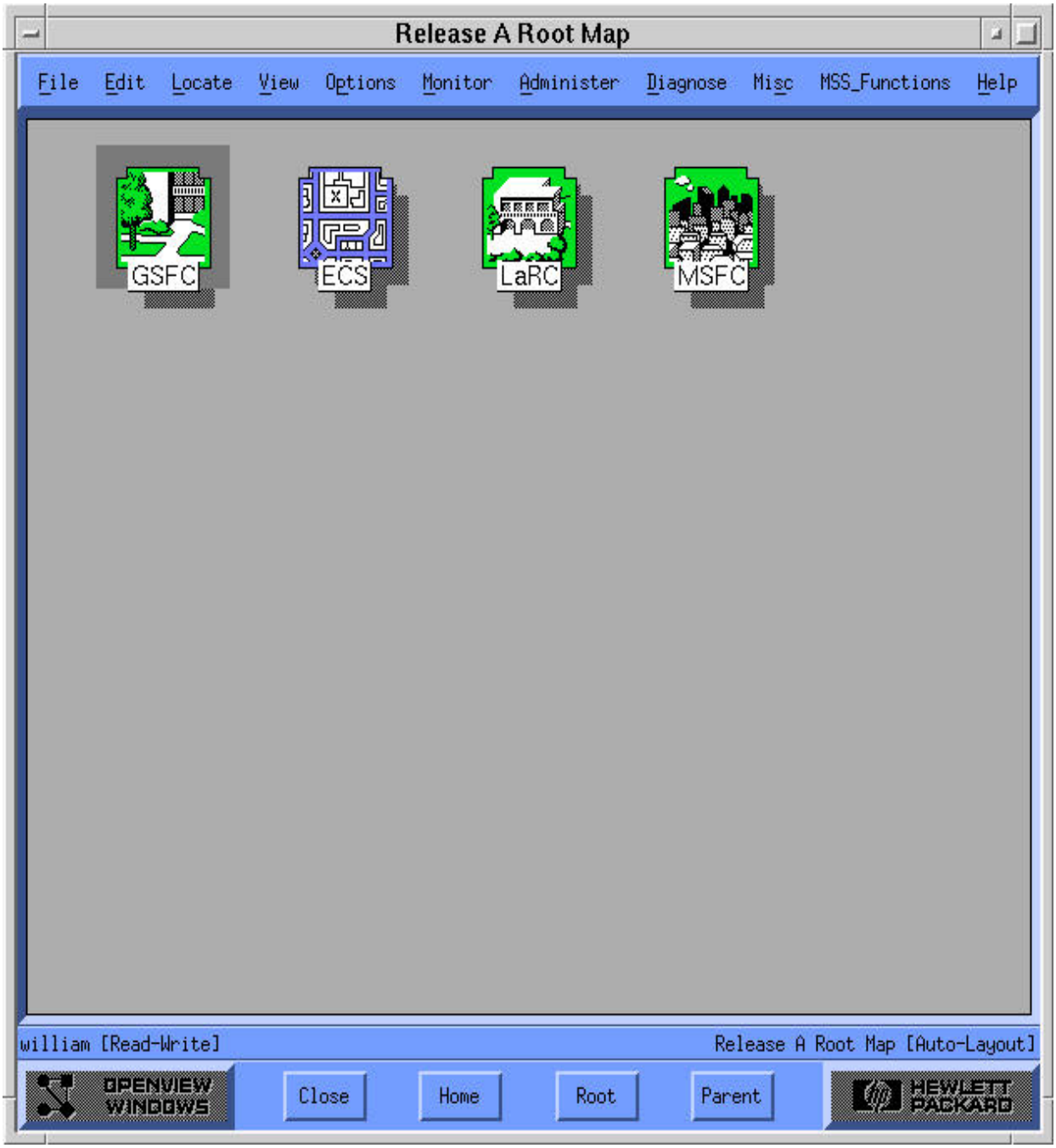

Figure 3.6.1.6-1. HP OpenView Release A Root Map

Figure 3.6.1.6-2. HP OpenView Event Categories

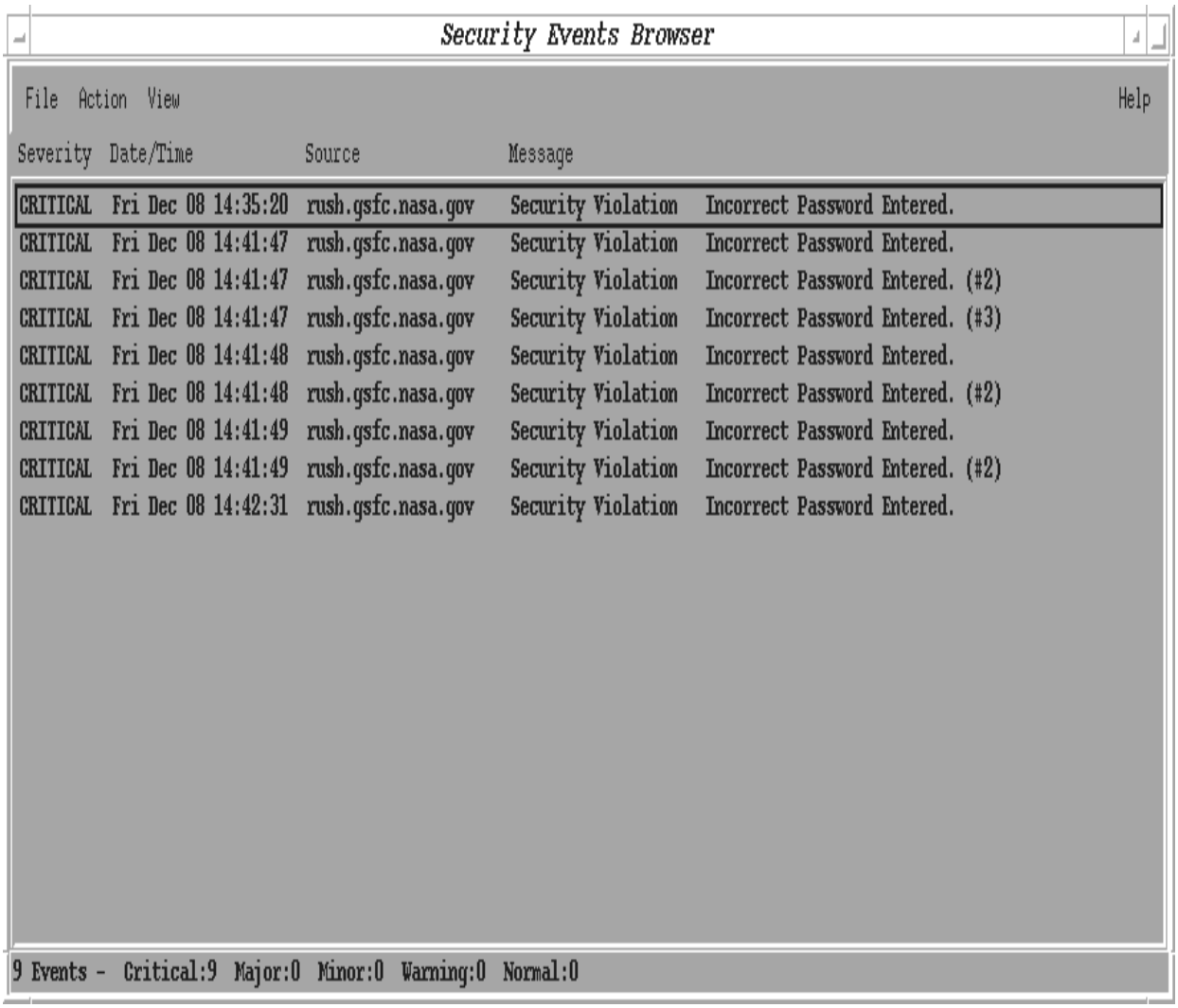

Figure 3.6.1.6-3. Security Events Browser

3.6.2 Accountability Management Create User Account Scenario

3.6.2.1 Scenario Description

This scenario describes the lifecycle for User Account Creation from the user filling out the User Registration Request form to the user logging into ECS with their new account. In this example, a potential ECS user fills out a request to receive an ECS Account. The involved staff are the DAAC Computer Operator, The DAAC Review Panel and the User Services Personnel. The responsibilities and roles of these staff members are described in the Maintenance and Operations Manual for the ECS Project (607-CD-001-001) and/or The Maintenance and Operations Configuration Management Plan for the ECS Project. In this scenario a potential user fills out and submits a registration form. The DAAC Operator then delivers a list of potential users to the DAAC User Registration Review Panel. The panel then review the requests and approves or disapproves the new users. The panel fills out an approval sheet (files for records) and passes the request onto the User Services group. The User Services group then updates the account with the appropriate information and submits the account to be created. The user then receives notification of the account and successfully logs into the system.

3.6.2.2 Frequency

During the initial three months of operations we expect a higher (25-30 per day) amount of user account request. After this we expect a downward slope leveling off at about 5 requests per day. A user may fill out and submit a Registration Request form at any time. The operator will query the pending account information (at a time to be determined by the individual DAACs).

3.6.2.3 Assumptions

The assumptions underlying this scenario are as follows:

1. The time to query the pending accounts is a DAAC dependent variable that will be determined by the individual DAACs.
2. The individual requesting the account will have a US Mail Box or Post Office Box to receive the available account information.
3. The user will supply a verification key (i.e., mothers maiden name), this will be used in the case of a user who has forgotten their password.

3.6.2.4 Components

The other subsystem involved with this activity is CSS. Please see Screen dumps of forms and requests for additional components.

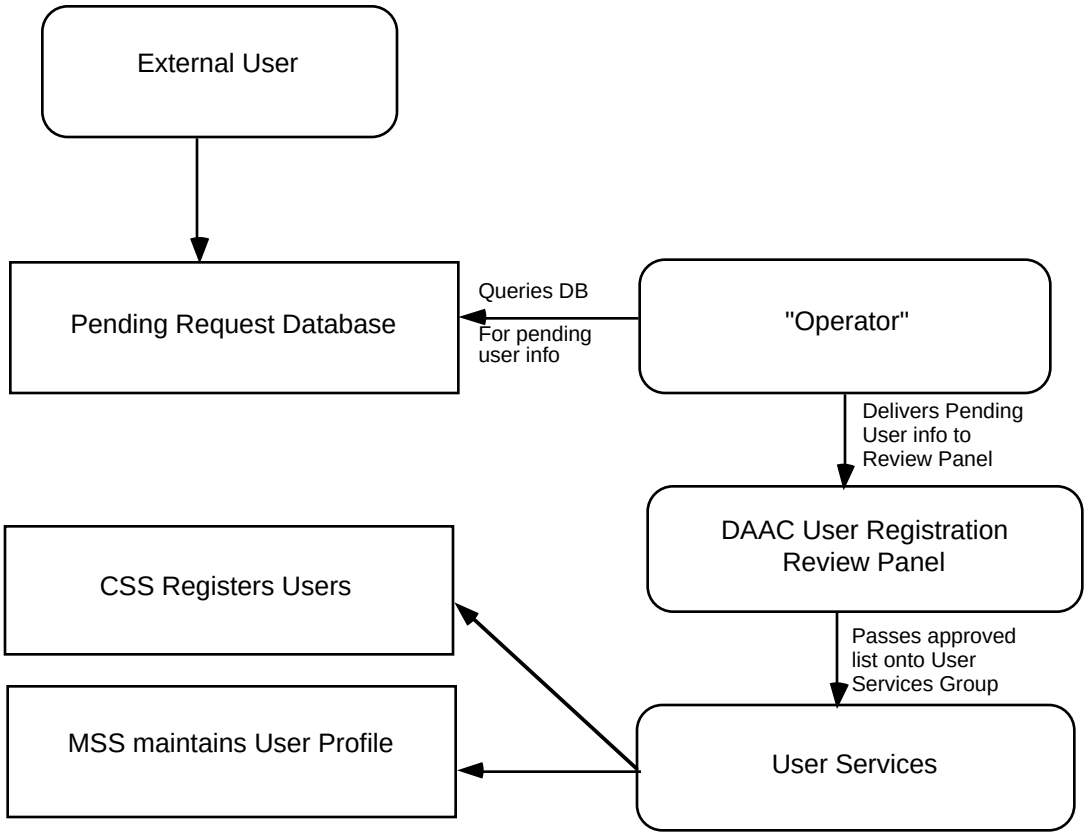

Figure 3.6.2.4-1. Accountability Management Create User Account Components

3.6.2.5 Preconditions

The following preconditions are assumed for this scenario:

1. A potential user has submitted an ECS User Registration Form.
2. The operator has check the query to see if any new requests exist.

3.6.2.6 Detailed Steps of Process

Table 3.6.2.6-1 represents the details of this scenario. The times and duration given are approximate.

Table 3.6.2.6-1. Accountability Management Create User Account Process (1 of 3)

Step	Duration	User Action	Operator Action	System	Figure
1	5 Time = 1105	User Fills out ECS User Registration html and submits it.			
2	< 1 Time = 1106			Stores the user request information into the Pending Request Database and spawns an html back to the user. This html notifies the user that the information has been stored into the database and that the account approval is pending	
3	< 1 Time = 1106	User receives html back from the system notifying the user that there information has been stored and that it is pending approval.			
4	3 Time = 1400		DAAC Computer Operator performs a query on the Pending Request Database to retrieve a list of pending user registration requests. (Screen provided below).		3.6.2.6-1
5	< 1 Time = 1401		DAAC Computer Operator delivers the list of pending user registration requests to the DAAC User Registration Review Panel.		
6	30 Time = 1431		DAAC User Registration Review Panel reviews each of the requests and approves or disapproves the new user account. Some of the key items considered by the review board are: affiliation, sponsor, reason, etc.		

Step	Duration	User Action	Operator Action	System	Figure
7	2 Time = 1433		DAAC User Registration Review Panel sends the new account information to the User Services group. Review Panel fills out and signs approval sheet and keeps this sheet on file for future reference. (Approval Sheet provide below).	Sends message back to user notifying them that their account has been approved and that they will receive notification in the US mail within 5 days.	3.6.2.6-2
8	< 1 Time = 1434	User receives email notification that the account has been approved and that further information will follow in the US mail			
9	10 Time = 1445		User Service Group then updates each account with the appropriate information, i.e., user id and password (the password will only show up as asterisks).		
10	1 Time = 1446		User Services Group then clicks on submit to create the account		
11	< 1 Time = 1447		User Services Group retrieves the US Mail message and delivers it to the outgoing mail (where it will be picked up by the US Post Office).	Approves and generates new account. Account information is stored in the User Accounts Database. A US Mail message containing account information automatically generated.	

Step	Duration	User Action	Operator Action	System	Figure
12	3-5 days	Receives US Mail message with account information. This information includes a password that will expire after one use. Thus forcing the user to change their password immediately.			
13	< 1 Time = 0800	Verifies (by logging into ECS) that the account information is valid.			

3.6.2.7 Postconditions

The users that have requested for ECS accounts will have received a response back notifying them if there account has been approved. Those accounts that have been approved will be able to log into ECS.

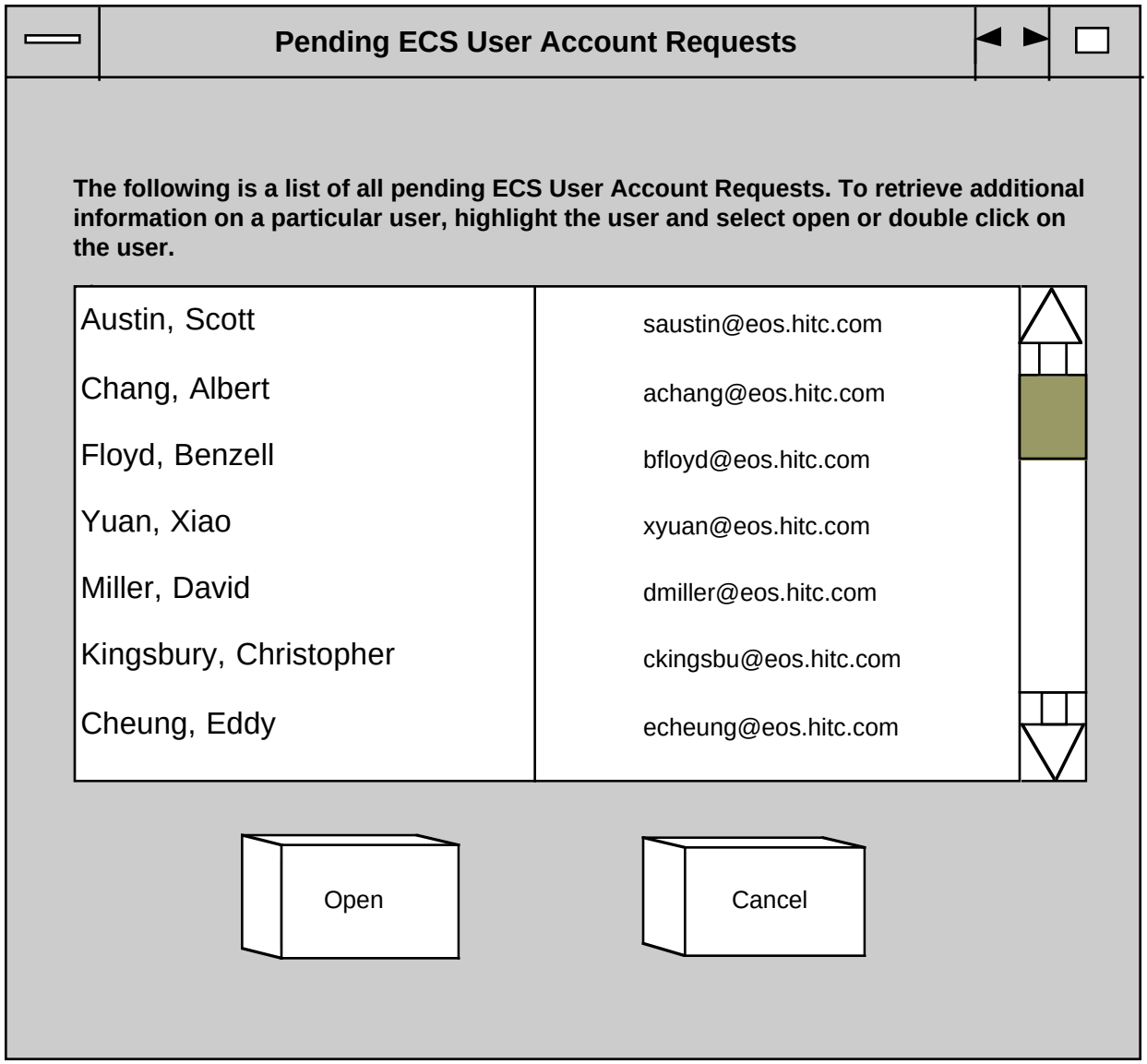

Figure 3.6.2.6-1. Pending User Account Requests

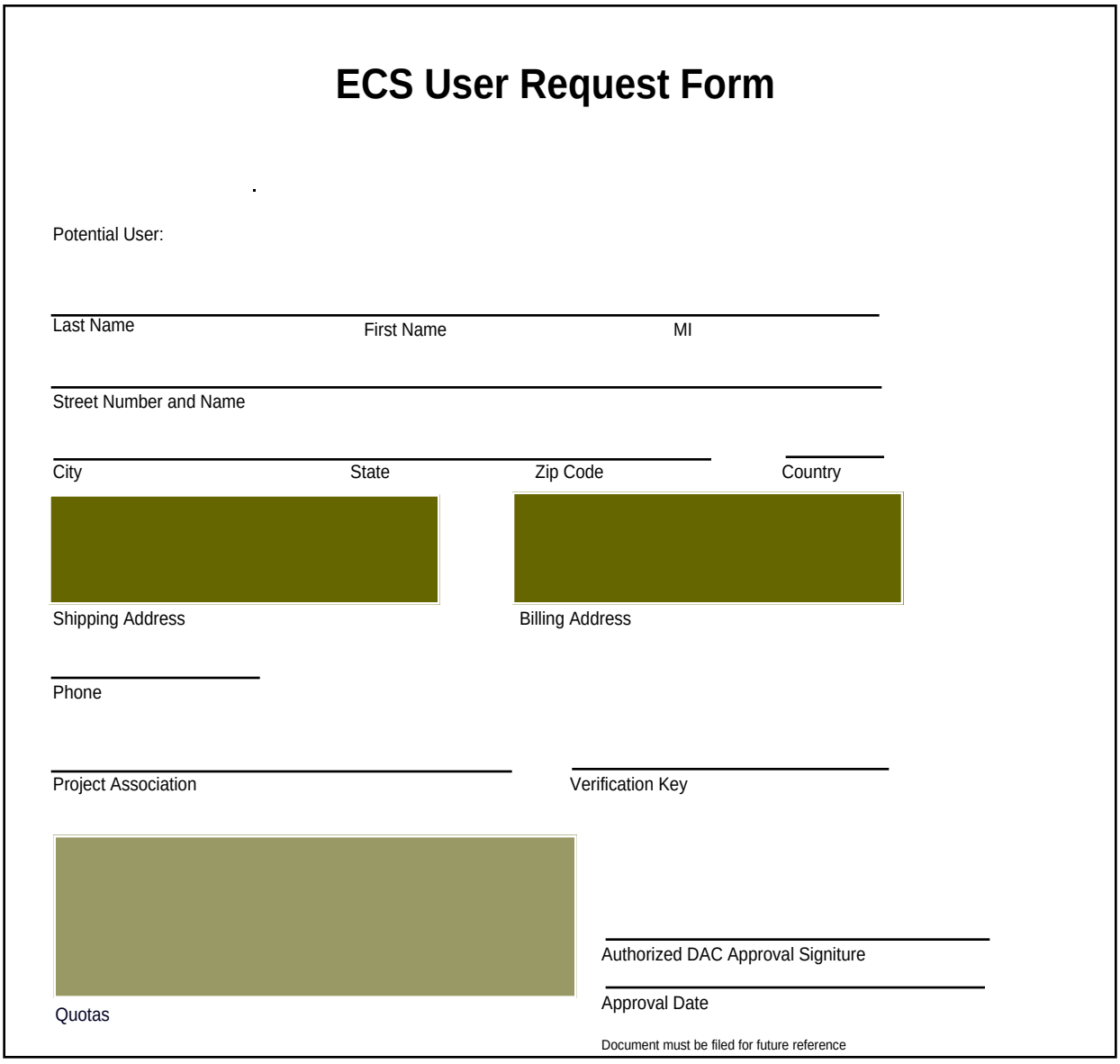

Figure 3.6.2.6-2. ECS User Request Form